DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 6-3: Personal Data Assistants and Communication Devices

1. References.

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

   i. III Corps Blackberry Policy, 19 August 2005.

2. Purpose of Policy: The purpose of this policy is to create a healthy balance between productivity improvements available through portable devices and maintaining risk management of trusted resources.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

   a. Commanders, directors, and supervisors at all levels shall ensure that subordinate personnel are aware of their individual responsibilities to protect these valuable resources and use them in an authorized and effective manner.

   b. Users of automated information systems (AIS) will use automated resources responsibly and abide by normal standards of professional and personal conduct at all times.

   c. All 4ID personnel and tenants shall report suspected unauthorized activity to their respective Information Assurance Manager (IAM), Information Assurance Network Manager/Officer (IANM/O), or Information Assurance Security Officer (IASO).

5. New Technology Steering Committee:

a. The 4ID Information Assurance Manager (IAM) shall organize and lead a 4ID Steering Committee to guide the evaluation of benefits, risks, and connectivity solutions for portable computer and communications tools.

b. This steering committee shall consist of technical experts from the respective 4ID service provider organizations and user representatives from the respective 4ID customer sites.

c. It is the responsibility of this committee to identify emerging portable tools, confirm user requirements and benefits, document inherent IA risks, and collaborate in assessing, testing, and recommending best of breed solutions permitting connectivity to trusted resources.

d. The purpose of this steering committee is to collaborate at the 4ID (versus site) level to compress learning curves, shorten implementation cycles, and gain productivity improvements while protecting the trust requirements of 4ID automated information systems (AIS) and communications resources.

6. Policy:

a. It is a directive of this policy that no portable devices will be connected to or interfaced with trusted 4ID AIS unless pre-approved by the New Technology Steering Committee using connectivity methods tested and validated (or accepted by this steering committee) as being effective.

b. Government purchased PDA's will be accredited by the appropriate DAA. Users of the devices must follow the accreditation instructions at all times. PDAs will not be taken into SCIFs without the approval of the local Special Security Officer (SSO). If the PDA either gets attached to a classified system or otherwise processes or stores classified information the device must then be stored in an approved storage area at all times the device is not in the possession of the user. The approved storage area must be accredited for the highest level of classification of the system to which it was attached or the information the device processed or stored.

c. Personally owned PDA's are not authorized and may not be connected to government information systems. Violation of this will result in confiscation until the hard drive is wiped/purged by IA personnel.

d. PDA technology is evolving and software is being developed that enhances the security of these devices. On certain PDA's (e.g., Palm Pilot), third party software is available that encrypts the content stored on the device, and password protects access to the device. Similarly, wireless communications devices are not secure by default. Wireless Application Protocol (WAP) is the communication standard for wireless applications. WAP security issues are being addressed through third party enhancements that provide transport layer security. The technology is very young and needs additional development. Currently, PDA's have not been approved for use with sensitive but unclassified information. If any command has a functional requirement for PDA or wireless communication technology for PDA's, contact the 4ID IAM for guidance on using and securing these devices. 4ID Commands, Garrisons, and Tenants are advised not to use PDA technology until it can be adequately secured.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding